Consent - the key concept that simply does not work

Svantesson, Dan Jerker B; Sak, Terrance

Published in:
Privacy Law Bulletin

PRIVACY LAW BULLETIN

Consent – the key concept that simply does not work[1]

Dr Dan Jerker B Svantesson[2] *and* ***Terrance Sak***[3] *BOND UNIVERSITY*

Consent is a key concept in much of the world's various privacy regulations. One finds it in the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[4] *it plays a pivotal role in the Asia Pacific Economic Cooperation (APEC) Privacy Framework*[5] *and in the privacy laws of many countries, such as Australia.*[6]

The relevance of the concept of consent is typically such that consent works like a miracle cure for any alleged privacy violation. If a data controller has obtained the data subject's consent, it may, for example, use and/or disclose personal data it otherwise would not be entitled to use and/or disclose.[7] Further, it may transfer personal data to a third country where such a transfer would not otherwise be allowed.[8]

Despite its widespread use in privacy regulation, legitimate questions have been raised for years regarding the appropriateness of how consent is gained from data subjects.

While the details of the type of role that consent plays varies from jurisdiction to jurisdiction, this article identifies three common aspects of consent in privacy law that are unsatisfactory. First, consent is not always required when it ought to be. Second, where consent *is* (emphasis added) required, the requirements are too easy to satisfy; that is, the benchmark for an acceptable consent is inadequate. Finally and closely related is the practical difficulty of actually enforcing the legal requirement for consent.

Consent not required when it ought to be

Currently, consent is typically never "the only basis for permitting the handling of personal information in a particular way".[9] Instead, privacy regulations commonly only utilise consent *as an exception* (emphasis added) to certain prohibitions, for example, the collection of sensitive information, use or disclosure for a secondary purpose, and cross-border transfer of information.[10] But is there really no circumstance under which consent should not be made the *only prerequisite* (emphasis added)? In other words, are there no circumstances in which it is reasonable to demand consent, and simply make the relevant data use unlawful where no consent has been obtained?

Direct marketing is one interesting area in this context. Looking at Australia, we note that, while not favoured in the end (presumably due to the expected increase in compliance costs),[11] the Office of the Federal Privacy Commissioner (OPC) considered requiring explicit consent *before* (emphasis added) an organisation is allowed to use or disclose personal information for the purposes of direct marketing.[12] After all, the Australian Spam Act 2003 prohibits spamming — which is frequently done for direct marketing purposes — unless there is prior consent.[13]

This inconsistency between the privacy legislation and the spam regulation is made possible by the fact that the definition of personal information is yet to extend to information from which its subject is merely contactable — a spam message can be effected with, for example, only an e-mail address, which may fall outside the definition of personal information.

Looking at the ongoing privacy reform in Australia, the draft Australian Privacy Principle 7 (exposure draft of privacy reform) — which deals particularly with direct marketing — does not make consent a necessary precondition to the use or disclosure of non-sensitive personal information for direct marketing purposes.

Perhaps the current stance reflects the arguable truth in the movement that "information wants to be free", especially in this digital age. But should the need for consent be discarded — and thus privacy less protected — simply to reduce compliance costs in furthering a relatively non-essential purpose such as direct marketing?

Consent requirements too easy to satisfy

While the definitions vary, a valid consent must typically comprise of two main elements: "knowledge of the matter agreed to, and voluntary agreement".[14] In e-commerce, the contradictions with these requirements

are prevalent. The wide use of lengthy standard form contracts results in e-consumers rarely having full knowledge of what they consented to, and frequently leaves them with little choice but to consent if they desire the underlying goods or services. In other words, goods and services, and the associated terms and conditions decided by the provider, are provided on a "take it or leave it" basis.

Further, the common use of a single "I accept" button for a mountain of various terms reduces the likelihood that e-consumers full-heartedly agree with all the proposed terms. While any potential solutions are likely restricted by the nature and manner in which e-commerce is currently conducted, this type of bundled consent can never be acceptable in relation to a basic human right like privacy.

The Australian Law Reform Commission (ALRC) was at pains to emphasise that the form of consent required is "often highly dependent on the context in which personal information is collected, used and disclosed".[15] In the context of e-commerce then, the non-compliance mentioned above may be given less weight in determining the validity of a purported consent. It is hoped that in accordance with the ALRC's recommendation,[16] the OPC will provide guidance which is particularly relevant to internet transactions.

Another element of consent is that the person whose consent was purportedly given must have the mental and legal capacity to consent. For e-commerce, anonymity on the internet raises an immediate problem — since e-retailers are seldom in a position to determine their customers' capacity, how can they ensure that this element was met? The OPC stated that despite the requirement, "an organisation can ordinarily assume capacity unless there is something to alert it otherwise".[17] If this is followed, then the anonymity *itself* (emphasis added) defeats the peculiar problem that it posed — since an e-retailer is usually unable to determine its customers' capacity, it is unlikely to be alerted to any lack of capacity. It follows then that there is almost no threshold for an e-retailer to satisfy this element. This said, it is unclear whether the OPC had internet transactions in mind when it so clarified. Understandably, a retailer who can observe its customers has proper basis to assume capacity where no opposite signs are shown; but where the customer can only be perceived through its online credentials, there is no basis for either position — thus, the presumption of capacity is less justified.

In light of the above, a special onus should be placed on e-retailers to determine the capacity of its prospective customers prior to contract. While this may seem impractical at present, Clarke's suggestion of a mechanism for "e-consent" provides a good starting point.[18]

Difficulty enforcing the requirement for consent

A requirement of consent will have no practical force if the data subject does not know of the related action (collection, use or disclosure, trans-border transfer) in the first place. Similarly, due to the complaint-driven model of, for example, Australia's Privacy Act 1988 (Cth), the requirement will be unenforced if the affected data subject does not know of the need to consent.

In Australia, these possibilities are not purely hypothetical. In certain circumstances for example, a requirement for consent can be bypassed based on it being "impracticable for the organisation to seek the individual's consent".[19] However, if it is impracticable to seek consent, then it might well be that any communication to the data subject informing of the data collector's conduct or the data subject's rights will not actually come to the attention of the data subject. Consequently, enforcement will rarely be carried out. Hence the better approach, notwithstanding any "impracticabilities", is for privacy regulation to ensure that the affected data subjects are properly informed of the related action — if it is equally "impracticable" to inform the data subject that its right to consent has been circumvented then the action itself should be abandoned.

Concluding remarks

Summarising the above, our rather sad conclusion is that the concept of consent — so central to privacy regulation around the world – simply does not work. It makes sense in theory, but the practical application of the concept illuminates its flaws. First, consent is not always required where it should be required. Second, it is too easy for businesses and organisations, particularly in the online context, to obtain consent, and consent given in such circumstances is meaningless. Third, the enforcement of consent-based schemes is often displaced where the data subject is unaware of the consent requirement.

To this we can add that, when one looks at the consent regulation from the perspective of business operators and organisations bound by privacy regulations, it becomes clear that obtaining and tracking consent is costly and cumbersome.

Combining these observations, it seems possible to conclude that the consent framework found in privacy regulations around the world is costly for business and has the effect of negating the positive effect of substantive privacy laws.

Dan Jerker B Svantesson,
Associate Professor, Faculty of Law, and
Terrance Sak,
Law Student, Faculty of Law,
Bond University.

Footnotes

1. Research for this paper was funded by a generous grant from the .auDA Foundation.
2. Associate Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, E-mail: Dan_Svantesson@bond.edu.au, (www.svantesson.org).
3. LLB Candidate at Bond University.
4. 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Preface www.oecd.org/ (accessed 10 August 2010).
5. www.apec.org/, (this can be accessed by clicking on media releases/2004/Ministers Endorse Privacy Framework) (accessed 12/4). For a more detailed discussion of the APEC framework, see: Carla Bulford, Between East and West: The APEC Privacy Framework and the Balance of International Data Flows 3 ISJLP 705 2007–08.
6. Privacy Act 1988 (Cth).
7. Above at NPP 2.1(b).
8. Above at NPP 9(b).
9. ALRC Report 108 19.3.
10. Above at 19.4–19.7.
11. Office of the Federal Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provision of the Privacy Act 1988* (2005), 103; recommendation 23 was silent on requiring explicit consent.
12. Above at [102].
13. Spam Act 2003 (Cth) s 16.
14. Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 22.
15. ALRC Report 108 19.59.
16. Above, Recommendation 19-1.
17. Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 22.
18. <http://www.rogerclarke.com/EC/eConsent.html> 27 July 2010.
19. For example, Privacy Act 1988 (Cth), NPP 2.1(c)(i).